TL

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,663	02/07/2002	Dongfeng Jing	08212/000S007-US0	3310

38879 7590 09/19/2006

DARBY & DARBY P.C.
P.O. BOX 5257
NEW YORK, NY 10150-6257

EXAMINER	
POWERS, WILLIAM S	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 09/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/072,663	JING ET AL.	
	Examiner	Art Unit	
	William S. Powers	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____:

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/7/2006 has been entered.

Response to Arguments

1. Applicant's arguments, see Remarks page 1, filed 7/7/2006, with respect to the rejection(s) of claim(s) 13-20 under 35 USC 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further search and consideration, a new ground(s) of rejection is made in view of WO 2001/26322 to Khalil et al. (hereinafter Khalil).

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

4. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

5. Claims 1-3 and 13-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over WO2001/26322 to Khalil et al. (hereinafter Khalil) in view of US Patent No. 6,948,074 o Borella et al. (hereinafter Borella) in still further view of US Patent Application No. 2001/0016492 to Igarashi et al. (hereinafter Igarashi).

As to claim 1, Khalil teaches:

a. An MN that is configured to generate a Reg-Req message (Khalil, page 12, lines 15-22) that includes Diffie-Hellman parameters that are used to generate session keys (Khalil, page 23, lines 4-7).

Khalil does not expressly mention the use of signatures in the secure messaging system of the invention. However, in an analogous art, Borella teaches producing signatures using the Diffie-Hellman protocol (Borella, column 10, lines 38-42).

Therefore, it would have been obvious at the time the invention was made to implement the mobile node registration of Khalil with the Diffie-Hellman signatures of Borella in order to provide an authentication parameter within the message.

b. Initiate an authentication session by sending the Reg-Req message (Khalil, page 12, lines 15-22).

c. Receive a Reg-Reply message that includes session keys that may be used to directly communicate with the AAAH, AAAF, HA, and FA nodes while the MN is in a foreign authority, wherein the session keys are encrypted and wherein the session keys include a first at least one key, a second a least one key, and a third at least one key (Key 0, Key 1 and Key 3 are used by the MN to communicate with the other entities) (Khalil, page 13, lines 20-32).

d. An FA that is configured to receive the Reg-Req message (Khalil, page 12, lines 25-28).

e. Ensure that the authentication session is valid and when valid, sign and send the Reg-Req message; otherwise, end the authentication session (using MD5 as a security standard in communications between entities) (Borella, column 10, lines 35-48).

f. Receive, and authenticate (Borella, column 10, lines 35-48) the Reg-Reply message decrypt at least one key of the session keys sign, and send the Reg-Reply message to the MN (the session key is in unencrypted form, but is sent over a secure communications pathway that resulted from IKE protocol to protect the session key for the FA from detection) (Khalil, page 13, lines 20-30).

g. An AAAF that is configured to receive (Khalil, page 18, lines 13-22) and authenticate (Borella, column 10, lines 35-48) the Reg-Req message.

Khalil as modified does not expressly mention the AAAF generating session keys. However, in an analogous art, Igarashi teaches generating a first at least one of the session keys, by the AAAF, using the Diffie-Hellman algorithm and the Diffie-Hellman parameters (Igarashi, page 13, paragraphs 267-269).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the mobile node registration of Khalil as modified with the session key generation of the AAAF of Igarashi in order to distribute network device data over different networks as suggested by Igarashi (Igarashi, page 1, paragraph 1).

h. Add an identifier relating to the Reg-Req message (Borella, column 10, lines 35-48).

i. Sign and send the Reg-Req message (Borella, column 10, lines 35-48).

j. Receive, authenticate, sign (Borella, column 10, lines 35-48) and send the Reg-Reply message to the FA (Khalil, figure 13d).

k. An AAAH that is configured to receive and authenticate the Reg-Req message (Borella, column 10, lines 35-48).

l. Generate a second at least one key of the session keys (Khalil, page 19, lines 12-23).

m. Sign and send the Reg-Req message (Borella, column 10, lines 35-48 and Khalil, page 19, lines 3-11).

n. Receive and authenticate the Reg-Reply message (Borella, column 10, lines 35-48 and Khalil, figure 13d).

o. Generate a third at least one key of the session keys (Khalil, page 19, lines 12-23).

p. Encrypt the session keys (Khalil, page 19, lines 12-23).

q. Sign and send the Reg-Reply message to the AAAF (Borella, column 10, lines 35-48 and Khalil, figure 13d).

r. An HA that is configured to receive the Reg-Req message (Khalil, page 19, lines 12-23).

s. Prepare a Reg-Reply message in response to the Reg-Req message (Khalil, figure 13d).

t. Send the Reg-Reply message to the AAAH (Khalil, figure 13d).

As to claims 2 and 18, Khalil as modified teaches the Diffie-Hellman parameters include an n, a g, and a p parameter, wherein the parameters are used to generate the session keys (Khalil, page 23, line 1-page 24, line 4) and are used in signing the Reg-Req message and the Reg-Reply message (Borella, column 10, lines 35-48).

As to claim 3, Khalil as modified teaches wherein the Reg-Req message and the Reg-Reply message include an identifier relating to where the message originated, wherein the identifier is selected from an NAI (Khalil, page 14, lines 22-27).

As to claim 13, Khalil as modified teaches:

a. Establishing secure associations between a MN, an AAAH, an AAAF, a HA, and a FA to help ensure secure communication (Khalil, page 20, lines 12-32).

b. Securing a Reg-Req message and a Reg-Reply message used in establishing the secure associations (Khalil, pages 12-14).

c. Creating a plurality of session keys by the AAAH (Khalil, page 19, lines 12-23) and at least another session key by the AAAF (Igarashi, page 13, paragraphs 267-269).

d. Distributing the session keys in a secure manner (Keys are distributed through the security associations) (Khalil, page 20, lines 12-32).

As to claim 14, Khalil as modified teaches using a home authority and a foreign authority to maintain and help establish the secure associations (Khalil, pages 12-14).

As to claim 15, Khalil as modified teaches:

a. Establishing a secure association between the MN and the AAAH (Khalil, page 16, line 19-page 17, line 21 and figure 12).

b. Establishing a secure association between the AAAH and the HA (Khalil, page 16, line 19-page 17, line 21 and figure 12).

c. Establishing a secure association between the AAAF and the AAAH (Khalil, page 16, line 19-page 17, line 21 and figure 12).

d. Establishing a secure association between the AAAF and the FA (Khalil, page 16, line 19-page 17, line 21 and figure 12).

e. Establishing a secure association between the AAAF and the MN (Khalil, page 16, line 19-page 17, line 21 and figure 12).

As to claim 16, Khalil as modified teaches determining when a signature is an authentic signature based on the secure associations and the session keys (Borella, column 10, lines 35-48).

As to claim 17, Khalil as modified teaches:

a. Signing the Reg-Req message and the Reg-Reply message using the session keys (Borella, column 10, lines 35-48).

b. Authenticating the received Reg -Req message and the Reg-Reply message (Borella, column 10, lines 35-48).

6. Claims 4-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over WO2001/26322 to Khalil et al. (hereinafter Khalil) in view of US Patent No. 6,948,074 o Borella et al. (hereinafter Borella) in still further view of US Patent Application No. 2001/0016492 to Igarashi et al. (hereinafter Igarashi) as applied to claim 3 above, and further in view of US Patent Application No. 2002/0062385 to Dowling et al. (hereinafter Dowling).

As to claim 4, Khalil as modified teaches signing the messages, but does not expressly mention the security associations signing the messages between the nodes of the networks. However, in an analogous art, Dowling teaches messages are signed using a security association between a sender of the message and the message receiver message (Dowling, paragraph 116).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the mobile node registration of Khalil as modified with the security association signatures of Dowling in order to make the message unreadable to third parties as suggested by Dowling (Dowling, paragraph 116).

As to claim 5, Khalil as modified teaches wherein the AAAF is further configured to choose a secret random number y to calculate a parameter $q = g^y \bmod n$ according to the Diffie-Hellman algorithm that is used in generating the session keys (Khalil, page 23, line 1-page 24, line 4).

As to claim 6, Khalil as modified teaches authenticating the Reg-Req message and the Reg-Reply message further comprises ensuring that the Reg-Req message and the Reg-Reply message came from the sender by checking the signature relating to a security association between the sender and the receiver (Dowling, paragraph 116).

As to claim 7, Khalil as modified teaches the AAAF is further configured to determine the AAAH for the MN in response to the identifier associated with the MN (Igarashi, paragraphs 128-130).

7. Claims 8-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over WO2001/26322 to Khalil et al. (hereinafter Khalil) in view of US Patent No. 6,948,074 o Borella et al. (hereinafter Borella) in further view of US Patent Application No. 2001/0016492 to Igarashi et al. (hereinafter Igarashi) and in still further view of US Patent Application No. 2002/0062385 to Dowling et al. (hereinafter Dowling) as applied to claim 7 above, and further in view of US Patent No. 6,915,345 to Tummala et al. (hereinafter Tummala).

As to claim 8, Khalil as modified does not expressly mention recording the time of the authentication session. However, in an analogous art, Tummala teaches the AAAF is further configured to store a time associated with the initiation of the authentication session in order to prevent a Reply message failure (Tummala, column 13, lines 7-12).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the mobile node registration of Khalil as modified with the recording of the time of the authentication session of Tummala in order to denote the acceptable lifetime of the authentication session as suggested by Tummala (Tummala, column 13, lines 7-12).

As to claim 9, Khalil as modified teaches the AAAH is further configured to protect the authentication process from a replay attack, and when the AAAH does not recognize the MN, generate an error (Borella, column 10, lines 5-34).

As to claim 10, Khalil as modified teaches the AAAH is further configured to help the FA directly communicate to the HA through a security association by generating the session keys for the FA, HA, and MN, and distributing the session keys in a secure fashion (generating the session keys and distributing them after setting up security associations between the various nodes) (Khalil, page 13, lines 20-32).

As to claim 11, Khalil as modified teaches distributing the session keys in a secure fashion, further comprises encrypting the session keys (Khalil, page 13, lines 20-32 and page 22, lines 8-13).

As to claim 12, Khalil as modified teaches wherein the HA is further configured to register a current location of the MN and store the session keys (Khalil, page 13, lines 9-30).

8. Claims 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over WO2001/26322 to Khalil et al. (hereinafter Khalil) in view of US Patent No. 6,948,074 o Borella et al. (hereinafter Borella) in still further view of US Patent Application No. 2001/0016492 to Igarashi et al. (hereinafter Igarashi) as applied to claim 18 above, and further in view of US Patent No. 6,785,823 to Abrol et al. (hereinafter Abrol).

As to claim 19, Khalil as modified teaches the Reg-Req message includes an NAI associated with the MN (Khalil, page 14, lines 22-27), a timestamp (lifetime) (Igarashi, paragraph 131) and the Diffie-Hellman parameters (Khalil, page 23, line 1-page 24, line 4). Khalil as modified does not expressly mention a FA challenge. However, in an analogous art, Abrol teaches a challenge issued by the FA as part of the Reg-Req message (Abrol, column 12, lines 1-5).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the mobile node registration of Khalil as modified with the FA challenge incorporated into the Reg-Req message of Abrol in order to improve authentication in a mobile network environment as suggested by Abrol (Abrol, column 1, lines 9-13).

As to claim 20, Khalil as modified teaches the Reg-Reply message includes an identifier and the session keys (Khalil, page 13, line 20-page 14, line 4 and page 14 lines 22-31).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent No. 7,042,879 to Eschbach et al. discloses the use of timestamps to prevent replay attacks.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to William S. Powers whose telephone number is 751 272 8573. The examiner can normally be reached on m-f 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on 571 272 6962. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

William S. Powers
Examiner
Art Unit 2134

9/11/2006

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100